

## Tips for Protecting Laptops and Portable Devices and Their Data

Produced by the California State ISO Office, July 2005

Every time a laptop computer (laptop) or other portable device (device) is lost or stolen, the data on that device has also been stolen. If state data is lost, accessed, or compromised as the result of a laptop theft, the resulting damage can be much greater than the cost of replacing the equipment.

Please take care to use your portable electronic equipment wisely. The tips below suggest ways to reduce the risk associated with ownership and transport of portable devices (laptop/device).

### Record identifying information and mark your equipment

- Record the make, model and serial number of the machine and any peripheral equipment. Keep these numbers in a safe place, away from your equipment, so if your laptop/device is stolen, the information will be available.
- Tag your laptop/device with identifying labels. Make sure it has a state inventory tag if it is state-owned equipment. If it is your private property, put a prominent label or other marking on it to identify it as yours. Vendors/consultants to the state should have their equipment clearly labeled.

### Protect your data

- Store all passwords, login instructions, and authentication tools separately from the laptop/device. Do not leave this information in the pockets of your carrying case or on the hard drive. This includes access codes and remote access phone numbers and account names.
- Back up your laptop/device data on a regular basis by copying data to removable media or by downloading critical files to your desktop or server. Protect the backup media appropriately. If the data that you are backing up is confidential, personal, and/or sensitive use special precautions to ensure that it is handled appropriately.
- Password-protect your laptop/device and the data that it contains. For layered protection, use separate passwords for your operating system and for individual applications. Use strong passwords, and do not share them with others. Numerous password tools and techniques are available. Your decision to use complex password schemes should be determined by the nature of the data on your machine and your ability to use the technology.
- Do an inventory of the data on your laptop/device, and classify it (SAM Section 4841.3 describes data classification categories). If your laptop/device contains confidential, sensitive, and/or personal data, you must take appropriate precautions to protect the data.

- You are responsible for protecting the integrity and confidentiality of the data for which you are a custodian. Encryption is a strong measure for protecting data. If your laptop/device contains confidential, sensitive, and/or personal data, you should consider encryption at rest to lower risk of data loss or compromise.

#### Physically protect your equipment

- Lock your laptop/device in a cabinet or drawer when you are not using it, or when you plan to be away from your desk. This simple practice can provide a lot of protection. Many office thefts are crimes of opportunity and are often committed by individuals who simply walk through buildings when few people are in the office.
- Use cable locking systems to anchor your laptop to a stationary object when appropriate.

#### Protect your laptop and other portable devices while traveling

- Keep your laptop in a satchel, brief case, or other nondescript bag. Standard cases designed specifically for laptops clearly announce their contents, making it easier for thieves to spot in crowded airports, restaurants, and conferences.
- Keep your laptop (or other device) out of sight when it is temporarily in a car, hotel room, or home. Keep it away from windows. Don't leave a laptop or other portable devices visible in unattended vehicles even for a moment. Make sure your vehicle doors are locked to secure the equipment. Laptops are frequently stolen from the trunks of cars, so don't leave your laptop in the trunk overnight or for extended periods.
- While commuting in a taxi, shuttle bus, or other public transportation, keep your laptop with you at all times. Do not permit a driver or baggage handler to load your laptop as baggage where it may be out of your view.

#### Be prepared with backup materials in case of laptop theft, loss, or destruction

- If you intend to use a laptop for a presentation or other critical activity, it is a good practice to print the slides as overhead transparencies, and to make paper copies of other important materials that you need for the activity. It is also a good practice to copy key data to removable media (flash drive or disk). Carry the copies separately, away from the laptop. If you have confidential, sensitive, or personal data on the removable devices, it is a good practice to encrypt the files.

#### What to do if your laptop is stolen

- If your laptop/device is stolen contact your department Information Security Officer (ISO) immediately. Your ISO will handle the security incident notification process (SAM Section 4845). **Alert your department ISO if the data contained on your stolen laptop/device is confidential, sensitive, and/or personal as described in SAM Section 4841.3.** If this is the case, a privacy breach notification may be necessary.